# Care Systems

# Cloud Infrastructure Technical Details

This document has been prepared to assist users of Care Systems software.
The information provided is general and may not be comprehensive for individual sites.
It is the Users responsibility to ensure that the process is completed satisfactorily.
Care Systems support services are available to assist should this be required.



**2024**

# Table of Contents

## Introduction

The Care Systems Cloud is a fully hosted management solution for the Aged Care industry. Care Systems manages all aspects of the technology solution and server licencing, allowing you to connect to the solution from any location and on any device.

This document provides technical and design details of the Care Systems Cloud solution.

# Technology, Infrastructure & Management

## Hosting Locations

- Care Systems Cloud services are hosted within Australian Tier 3+ data centres. These data centres provide minimum uptime of 99.982%, or a maximum of 1.6 hours of downtime annually.
- The primary services are located in Melbourne.
- Backup and disaster recovery services located in Canberra and Sydney.

## Technology Stack

### *Operating System*

- The Care Systems solution utilises a range of Microsoft Windows and Linux servers.
- All operating system and utility applications are regularly patched in line with OEM advice.

### *Data Security*

- All client information is encrypted at rest and in transit.

### *System Availability*

- Care Systems has maintained 99.9% uptime of our cloud-based services since 2015.

### *Threat Monitoring*

- Care Systems utilises real time remote monitoring of all server and service status to ensure system uptime is maintained.
- Industry best threat detection tools are used to provide real time intrusion prevention, antivirus, anti-malware, anti-ransomware, and log inspection.

## Backup and Disaster Recovery

### *Daily Backups*

- The entire solution is backed up to a remote location daily.

### *Disaster Recovery to Secondary Location*

- Disaster Recovery procedures are tested periodically to ensure system status can be re-established in a secondary data centre, in the unlikely event of a total data centre loss.

### *User Initiated Snapshots*

- Users can also initiate snapshots of a tenancy specific dataset to record the system state at a particular point in time.
- An example would be at the end of financial year or before a change in a tenant's corporate structure is applied to the system.

## Management Approach

- Care Systems utilises the ISO27001 framework to control our processes, products and systems.
- Care Systems has been assessed and is accredited under the ATO Operational Framework guidelines for organisational and system security for cloud-based solutions. More information on the ATO operational framework assessment process is available here:
  **https://softwaredevelopers.ato.gov.au/operational_framework**
- Care Systems adheres to the Australian Signals Directorate's "Essential 8" guidelines and is currently undertaking an assessment under the ASD's Information Security Registered Assessors Program (IRAP).
- More information on the IRAP program is available here:
  **https://www.cyber.gov.au/acsc/view-all-content/programs/irap**

## Administrative Access Control

- Administrative access is delegated to certified Care Systems staff and contractors on an individual basis.
- Access is suspended or revoked when an individual no longer requires administrative access to the system.
- Access levels are defined to grant the minimum required level of access to perform the required functions.
- Multifactor Authentication is required for all administrative accounts.

# Tenancy and User Access

## Common Tenancy Concepts

- Each client organisation is assigned a unique Tenant identifier within the Care Systems Cloud environment.
- A Tenant may be an Aged Care Provider Organisation, an intermediary such as an Accounting Firm or Bureau Service or another type of client organisation.
- Each person who accesses the system will have a unique User account. Each User account is associated with a primary Tenant and appropriate roles. Roles can be an Operator within the main Care Systems application, an Employee, a Client or a Supplier contact.

## Data Segregation by Tenant and Dataset

- All datasets are stored in separate database instances and accessed via separate connections with dedicated security per dataset.
- By default, each Tenant has access to a Live, Training, and Test dataset.
    - Live – live operations.
    - Training – a recent copy of the live dataset, which can be used to train staff while also being available to try new procedures.
    - Test – an area to perform user acceptance testing of new features before they are applied in the Live and Training areas.
- Other datasets can be configured within one tenancy as required. For example, a Tenant may have multiple companies and it is preferred these are managed separately, or additional non-live datasets are required for testing, training, reporting or other purposes.

## Grant Access to Users from Other Tenant Organisations

- In addition to managing your own users, other parties can be granted access to additional Tenant systems.
- These parties could be an employee of a bureau service or an accounting firm. You can grant them read+write access to the system, allowing them to process transactions or perhaps, read only access to generate reports and conduct audit activities.

## Dedicated Web Endpoint by Dataset

- Each dataset has dedicated endpoints for external access. Standard endpoints include:
    - API integration for employee, client financial data import and export from and to third parties.
    - Self Service web and application access for staff and other users.
    - Business Intelligence service access for reporting, dashboarding and custom data import and export.

## Application Patching

- All Application Updates are managed by Care Systems.
- Minor application updates will be applied after hours at an agreed time. No action is required by clients.
- Major application updates may require clients to complete user acceptance testing of new features to ensure continuity of operations following the update. An example of this requirement would be updates to client billing functions to implement changes in government policy.

## User Access Control

- Identity Management options can be configured on a Tenant by Tenant basis, and for groups of users within a Tenant. Options available in relation to identity management include:
    - Multifactor Authentication.
    - Users can be authenticated against your ADFS and SAML based identity management platforms.
- The level of access for each user can be controlled to a fine degree of detail. Users can be assigned to one or more Roles and each role can grant or deny access in the following ways:
    - Access to open menu items for each screen, report, and process within the system.
    - Access to individual sets of information within screens, such as denying access to Employee Tax information while granting access to other parts of the employee record.
    - Ability to view add, delete, update data can be controlled for each element.

# Client System Requirements

Client system requirements for accessing the Care systems solution include;

- Main application:
  - Computer or tablet running modern browser (e.g. Chrome, Firefox, Safari).
  - Computer or tablet capable RDP Published Application (Windows, macOS, iOS, Android).
  - Some main application screens are optimised for data entry using keyboard and mouse.
- Business Intelligence tools:
  - Computer or tablet running modern browser (e.g. Chrome, Firefox, Safari).
  - Optional Excel plug-in: Microsoft Excel running on a Windows based computer.
  - Third party system access via calls to RESTful API endpoints.
- RESTful API
  - Third party system access via calls to RESTful API endpoints.
- Employee Portal
  - Phone, Computer or Tablet running modern browser (e.g. Chrome, Firefox, Safari).